HIMSS Virtual Events

Industry advancing solutions.
Conveniently flexible formats.

HIPAA New Final Omnibus Rule: Key Implications for Your Organization

Speaker Bio

Adam H. Greene, JD, MPH

Davis Wright Tremaine, LLP
Partner

- Former Senior Health Information Technology and Privacy Specialist at HHS Office for Civil Rights
- Co-Chair, DWT Health Information Practice Group
- Chair, HIMSS Cloud Security Workgroup

Speaker Bio

Gerry Hinkley

Pillsbury Winthrop Shaw Pittman LLP
Partner

- Chair—HIMSS Legal Task Force
- Chair—Pillsbury Health Care Industry Team
- Member, eHealth Initiative Leadership Council

HIMSS Virtual Events

Learning Objectives

Industry advancing solutions.
Conveniently flexible formats.

- Learn about important clarifications regarding coverage of HIPAA to Business Associates and contractors
- Understand key new changes to the data breach notification standard,
- Prepare to operationalize key patient rights, such as access to electronic data, and right to restrict release of data to health plans

HIMSS Virtual Events

Agenda

Industry advancing solutions.
Conveniently flexible formats.

- Business Associates and Subcontractors
- Breach Notification Rule
- New Patient Rights
- New Limits on Uses and Disclosures
- Increased Enforcement
- Action Items

The Omnibus Rule

Finalizes the following:

- Interim final Breach Notification Rule (Aug. 2009)
- Genetic Information Nondiscrimination Act (GINA) modifications to HIPAA (proposed Oct. 2009)
- Interim final HITECH Act Enforcement Rule (Oct. 2009)
- HITECH Act privacy and security provisions (proposed July 2010)

HIMSS Virtual Events

What's Missing

Industry advancing solutions.
Conveniently flexible formats.

- HITECH Act Accounting of Disclosures/Access Report Rule (proposed May 2011)
- Guidance on minimum necessary standard
- Amendments to Clinical Laboratories Improvement Amendments (CLIA) and HIPAA (proposed Sept. 2011)
- Common Rule advance notice of proposed rulemaking (published July 2011)

HIMSS Virtual Events

Business Associates & Subcontractors

Industry advancing solutions.
Conveniently flexible formats.

- Omnibus Rule conforms HIPAA regulations to HITECH Act changes
  - Before HITECH, BAs regulated through business associate contracts or agreements ("BAAs")
  - After HITECH, BAs and subcontractors are regulated directly under HIPAA
    - Must comply with Security Rule (rule is flexible to accommodate small BAs)
    - Must comply with some of Privacy Rule and provisions of BAA

BAs – Expanded Regulation

- Expanded definition of "business associate“
  - “Business associate” means one who, on behalf of a covered entity, creates, receives, maintains or transmits PHI
  - "Business associate" now also means "subcontractor of business associate“ who creates, receives, maintains or transmits PHI on behalf of a business associate
  - Status as BA based upon role and responsibilities, not upon who are the parties to the contract
- Implications for subcontractor relationships
  - Contract between the covered entity's BA and that BA's subcontractor must satisfy the BA agreement requirements
  - Subcontractor of subcontractor is also a BA, and so on
  - As a result, HIPAA/HITECH obligations that apply to BAs also directly apply to subcontractors

BAs - Clarifications

- Rule clarifies definition of "business associate" -- included:
  - Patient Safety Organizations
  - Health information exchange organizations, e-prescribing gateways, covered entities' personal health record vendors (not all PHRs)
  - Data transmission providers that *require access to PHI on a routine basis*
- Not included – those who provide mere transmission services, like digital couriers or "mere conduits"
  - However, those who store PHI, even if they don't intend to actually view it, are BAs (implications for cloud model EHRs)

BAs – Uses of PHI

- Uses of PHI
  - BAs may use or disclose PHI only as permitted by BAA or required by law
  - BAs may not use or disclose PHI in manner that would violate Privacy Rule, if done by the covered entity
  - Subcontractors subject to limits in initial CE-BA agreement – must pass along in subcontracts
  - BAs not making a permitted use or disclosure if not following minimum necessary rules
- BA does not comply if it knows of subcontractor's material noncompliance and does not take reasonable steps to cure the breach or, if such steps fail, to terminate the relationship

HIMSS Virtual Events

BAs - Consequences

Industry advancing solutions.
Conveniently flexible formats.

- Secretary authorized to receive and investigate complaints against BAs (including subcontractors), and to take action regarding complaints and noncompliance
- BAs (incl. subs) required to maintain records and submit compliance reports to Secretary, cooperate in complaint investigations and compliance reviews, give Secretary access to information
- BAs (incl. subs) forbidden to intimidate, discriminate against, etc. those who make complaints, cooperate with regulators or oppose unlawful actions
- BAs (incl. subcontractors) subject to civil money penalties for HIPAA violations
- BA/Subs remain liable under contract to CE/BA

BAs – Transition Provisions

- Generally, compliance required 180 days following Omnibus Rule's effective date (3/26/13), which is 9/23/13
- Additional time allowed to enter into conforming business associate agreements (Limited Deemed Compliance Date)
  - If BAAs comply with pre-Omnibus rule, parties have 1 additional year to bring their BAAs into compliance with Omnibus Rule (9/22/14)
  - If BAAs do not comply with pre-Omnibus rule (or no BAA exists), must enter into BAAs that comply with Omnibus Rule by 9/23/13
  - Regardless of compliance deadlines, compliance with Omnibus Rule required when existing BAAs renew or are modified
  - BAAs not otherwise modified or renewed prior to 9/22/14 must be brought into compliance by that date

Breach Notification

- ~~"Significant risk of financial, reputational, or other harm"~~
- ~~Exception for limited data set without ZIP codes or dates of birth~~
- Presumption of reportable breach, unless ***low probability*** the PHI has been ***compromised*** after risk assessment

Breach Notification

Four required risk assessment factors:

1. Nature and extent of PHI involved
2. The unauthorized person who used the PHI or to whom the disclosure was made
3. Whether the PHI actually was acquired or viewed
4. The extent to which the risk to the PHI has been mitigated

Breach Notification

What is "compromised"?

The new rule doesn't say.

What is compromised?

- Center for Democracy and Technology/ Markle Foundation comment that suggested a "compromised" standard described it as "whether or not the data involved in the breach were at significant risk of being ***inappropriately viewed, re-identified, re-disclosed, or otherwise misused***"

Marketing Pre-HITECH

HIMSS Virtual Events

Industry advancing solutions.
Conveniently flexible formats.

- In public surveys of privacy concerns, marketing uses of data (esp. health and other sensitive data) rank very high
- Pre-HITECH: Marketing uses of PHI required prior patient authorization; however, communications sent by CEs for treatment or to recommend additional benefits or services were not marketing

Marketing – Omnibus Rule

HIMSS Virtual Events

Industry advancing solutions.
Conveniently flexible formats.

- Significant change from NPRM: prior authorization from patient required for using or disclosing PHI where the CE or BA receives financial remuneration for making a marketing communication from the third party whose product or service is being pitched
- Abandoned NPRM's distinction between communications for treatment and those for "operations;"
- If financial remuneration by or on behalf of the manufacturer whose product/service is being pitched to the covered entity or its business associate, the communication is marketing and requires prior patient authorization
- Authorization must disclose that the communication is paid for
- Covered entities can use a general authorization for all such communications or do it on a case-by-case basis

Marketing – Exceptions

HIMSS Virtual Events

Industry advancing solutions.
Conveniently flexible formats.

- Refill reminders exception
  - Subsidy allowed for currently prescribe drug or biologic; includes generics
  - Subsidy must be reasonably related to cost of making the communication (cannot make a profit)
- Face-to-face communications remain exempt with no requirement for any subsidy to be reasonable (related to labor, supplies and postage)
- Communication consisting of promotional gifts of nominal value provided by the covered entity remain exempt

What counts as "Financial "Remuneration"?

- Direct or indirect payments count; in-kind benefits do not count
- Payment must be for making the marketing communication; payments to implement programs (such as disease management programs) do not trigger marketing authorization requirements
  - Assumption is that the communication urges participation in the program, not the use or purchase of the third-party's product or service
- General health promotions or communications regarding eligibility for public programs – even if subsidized- are not marketing

Fundraising

Industry advancing solutions.
Conveniently flexible formats.

- Fundraising – use of PHI to promote the entity (not to benefit a third party)
- Expanded types of PHI able to be used for fundraising – includes department of service, treating physician, and outcome
- Requires clear and conspicuous opt-out, that must be honored
- Can notify of opt-out in initial communication; can do overall opt-out as well
- Cannot condition treatment on not opting out

HIMSS Virtual Events

Sale of PHI

Industry advancing solutions.
Conveniently flexible formats.

- Authorization generally required, with notice that disclosure of PHI is in exchange for payment; includes nonfinancial benefits
- Exceptions
  - Public health
  - Research purposes – remuneration must be reasonably related to the cost of preparing and transmitting information (can include indirect costs but cannot make a profit)
  - Treatment and payment – disclosure of PHI to receive payment is not a "sale" of PHI
  - Corporate transactions
  - Disclosures to business associates
  - Disclosures to the individual
  - Disclosures required by law
  - Other disclosures permitted by the rules, provided remuneration is related to cost of making the disclosure

Research

- Researchers have sought changes to both HIPAA and the Common Rule to ease the pathway to uses of data for research purposes
- Common Rule ANPRM released in July 2011
- Omnibus Rule includes a few provisions:
  - Allow remuneration for transfers of PHI for research (must be reasonable fee based on costs)
  - Allowance of compound authorizations
  - Authorizations no longer have to be study-specific; can have an authorization for future research as long as the description of the future research uses is sufficiently clear that it would be “reasonable for an individual to expect that his/her PHI could be used or disclosed for such future research”

Genetic Information – GINA

- Genetic Information Nondiscrimination Act of 2008 ("GINA")
  - Notice of Proposed Ruling (GINA Rule) October 7, 2009
- Prohibits genetic discrimination in health insurance and employment
- Rule implements GINA by:
  - Declaring genetic information (defined in GINA) to be PHI
  - Prohibiting most health plans covered by HIPAA from using or disclosing PHI that is genetic information for underwriting
  - Requiring plans to notify beneficiaries about this restriction in the NPP
- Exception for long-term care insurers, who can use genetic information for underwriting

Increased Patient Rights

Right of Access: Electronic Copy

- Individual continues to have right to copy of designated record set in the requested form ~~or~~ and format, if readily producible
- If not readily producible, then:
  - If designated record set is maintained electronically, individual has right to electronic copy (new)
  - If designated record set is maintained in hard copy, individual has right to hard copy

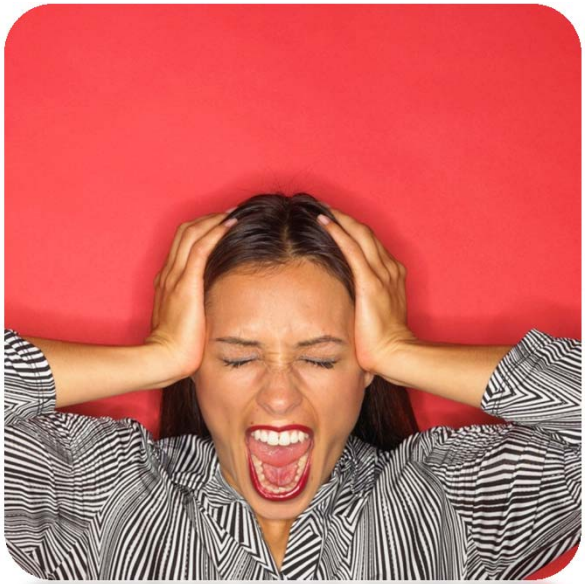
Increased Patient Rights

Right of Access: Copy to Third Party

- Individual may designate third party to receive copy
  - Must be in writing
  - Clearly identify the designated person
  - Clearly identify where to send the copy
- Access vs. Authorization: Who Is making the request?

Increased Patient Rights

Restriction for Out-of-Pocket Services



- Covered entity must agree to individual's request to restrict disclosure to health plan
  - For payment or health care operations
  - Unless disclosure is required by law
  - If individual (or 3rd party) pays for item or service out of pocket in full

HIMSS Virtual Events

Notice of Privacy Practices

Industry advancing solutions.
Conveniently flexible formats.

- Prohibition on sale of PHI
- Duty to notify affected individuals of a breach of unsecured PHI
- Right to opt out of fundraising (if applicable)
- Right to restrict disclosure of PHI when paid out of pocket
- Limit on use of genetic information (certain health plans only)

Enforcement

New Focus on Willful Neglect

- Willful neglect: Conscious, intentional failure or reckless indifference
- OCR will investigate all cases of possible willful neglect
- OCR will impose penalty on all violations due to willful neglect
- OCR may proceed to penalty without seeking informal resolution (e.g., settlement)

Enforcement

Other Changes to Enforcement

- Change in definition of “reasonable cause” (fills any gaps between “did not know …” and “willful neglect”
- Slightly revise factors to calculating civil monetary penalty
- Covered entities and business associates are liable for agents acting within scope of agency, even if business associate agreement is in place

HIMSS Virtual Events

Action Items

Industry advancing solutions.
Conveniently flexible formats.

- Revisit policies, procedures, and training
  - Consider approach for segregating out-of-pocket services
  - Opportunity for a HIPAA “tune-up”
- Revisit breach notification process
- Start using up those old notices of privacy practices

HIMSS Virtual Events

Action Items

Industry advancing solutions.
Conveniently flexible formats.

- Inventory BAs and update BAAs
- Train staff on new provisions
- Don’t delay

HIMSS Virtual Events

Thank You

Industry advancing solutions.
Conveniently flexible formats.

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213

Gerry Hinkley, JD

pillsbury

gerryhinkley@pillsburylaw.com
415-983-1135

HIMSS Virtual Events

Questions

Industry advancing solutions.
Conveniently flexible formats.